Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality

Ahmad R Pratama [Corresp., 1] , **Firman M Firmansyah** [2] , **Fayruz Rahma** [1]

[1] Department of Informatics, Universitas Islam Indonesia, Sleman, Daerah Istimewa Yogyakarta, Indonesia

[2] Department of Technology and Society, Stony Brook University, Stony Brook, New York, United States

Corresponding Author: Ahmad R Pratama
Email address: ahmad.rafie@uii.ac.id

Single sign-on (SSO) enables users to authenticate across multiple related but independent systems using a single username and password. While the number of higher education institutions adopting SSO continues to grow, little is known about the academic community's security awareness regarding SSO. This paper aims to examine the security awareness of SSO across various demographic groups within a single higher education institution based on their age, gender, and academic roles. Additionally, we investigate some psychological factors (i.e., privacy concerns and personality traits) that may influence users' level of SSO security awareness. Using survey data collected from 283 participants (faculty, staff, and students) and analyzed using a hierarchical linear regression model, we discovered a generational gap, but no gender gap, in security awareness of SSO. Additionally, our findings confirm that students have a significantly lower level of security awareness than faculty and staff. Finally, we discovered that privacy concerns have no effect on SSO security awareness on their own. Rather, they interact with the user's personality traits, most notably agreeableness and conscientiousness. The findings of this study lay the groundwork for future research and interventions aimed at increasing cybersecurity awareness among users of various demographic groups as well as closing any existing gaps between them.

1 # Security Awareness of Single Sign-On Account in the
2 # Academic Community: The Roles of Demographics,
3 # Privacy Concerns, and Big-Five Personality

5 Ahmad R. Pratama[1], Firman M. Firmansyah[2], Fayruz Rahma[1]

7 [1] Department of Informatics, Universitas Islam Indonesia, Sleman, DI Yogyakarta, Indonesia
8 [2] Department of Technology and Society, Stony Brook University, Stony Brook, NY, USA

10 Corresponding Author:
11 Ahmad R. Pratama[1]
12 Jl. Kaliurang Km 14,5, Sleman, DI Yogyakarta, 55584, Indonesia
13 Email address: ahmad.rafie@uii.ac.id

15 Abstract

16 **Background.** Single sign-on (SSO) enables users to authenticate across multiple related but
17 independent systems using a single username and password. While the number of higher
18 education institutions adopting SSO continues to grow, little is known about the academic
19 community's security awareness regarding SSO. This paper aims to examine the security
20 awareness of SSO across various demographic groups within a single higher education
21 institution based on their age, gender, and academic roles. Additionally, we investigate some
22 psychological factors (i.e., privacy concerns and personality traits) that may influence users' level
23 of SSO security awareness.

25 **Methods.** Primary data collected through an online survey from 283 participants (faculty, staff,
26 and students) at one of the largest private universities in Indonesia, analyzed using hierarchical
27 linear regression models.

29 **Results.** We discovered a generational gap, but no gender gap, in security awareness of SSO.
30 Additionally, our findings confirm that students have a significantly lower level of security
31 awareness than faculty and staff. Finally, we discovered that privacy concerns have no effect on
32 SSO security awareness on their own. Rather, they interact with the user's personality traits, most
33 notably agreeableness and conscientiousness. The findings of this study lay the groundwork for
34 future research and interventions aimed at increasing cybersecurity awareness among users of
35 various demographic groups as well as closing any existing gaps between them.

Introduction

37 Single sign-on (SSO) is a cybersecurity measure that enables the use of a single username and
38 password to authenticate the same user across multiple related but independent network,
39 computer, or information systems without having users enter their authentication credentials
40 multiple times. SSO enables end users to increase their productivity by significantly reducing the
41 time required for authentication processes (James et al., 2020). On the other hand, it may also
42 result in financial savings for the institution that implements it, for example, through cost savings
43 in their information technology expenditures (Chinitz, 2000; Gellert et al., 2019; Lane & Marie,
44 2010). However, it was not until the late 2000s that SSO adoption became more widespread in a
45 wide variety of organizations and enterprises, mainly due to performance issues (Lane & Marie,
46 2010) or insecure implementation (Bai et al., 2013) in its early days. Nonetheless, SSO adoption
47 was not uniform across sectors and regions of the world. Even in the early 2010s, some people
48 still refused to adopt SSO because they did not perceive an urgent need for it although that
49 perception changed as SSO's design and implementation improved (Sun et al., 2011).

50 There are numerous types of information systems in the academic community, particularly in
51 higher education institutions, including learning management systems (LMS), academic
52 information systems (AIS), management information systems (MIS), and payroll services. In
53 general, there are at least three distinct academic roles (i.e., students, faculty, and staff), each of
54 which usually has a different type and level of access to the institution's information systems.
55 Historically, colleges and universities required users to have separate accounts for each system.
56 This situation resulted in significant frustration for the users and increased support costs for the
57 institution. Implementing SSO resolves that issue by allowing users to log in to all systems using
58 the same username and password.

59 Along with the conveniences that SSO provides, there is an arguably greater risk associated with
60 the fact that that same account now has access to everything the user has access to. If attackers
61 gain access to an SSO account, they have the potential to cause additional damage, not just to the
62 user whose SSO account was compromised, but also to other users and the institution itself. Even
63 more so now that many universities have been forced to fully embrace online education in the
64 aftermath of the COVID-19 pandemic, forcing everyone, including those with limited online
65 experience, to quickly adapt to this digital transformation, the risk has increased. As a result,
66 safeguarding SSO accounts is becoming increasingly critical, even if not all users are aware of
67 such issues.

68 Numerous studies have been conducted on security awareness, including in the academic
69 community. However, little is known about the use of SSO in the academic community in
70 general, and even more specifically about users' security awareness regarding their SSO
71 accounts. This study aims to determine the level of security awareness among members of the
72 academic community regarding SSO accounts. We are particularly interested in examining the
73 psychological factors within individuals that can help predict their level of security awareness,

74 specifically their privacy concerns and personalities, and determining whether there is any
75 interaction between them. Additionally, we would like to determine whether the level of
76 awareness varies by demographic characteristics (e.g., age, gender) and academic roles (i.e.,
77 student, faculty, and staff). To be more precise, the term "staff" here refers to administrative
78 personnel, including librarians and technical support personnel, as opposed to non-administrative
79 personnel such as janitorial and security personnel.

80 The following section discusses our theoretical framework, beginning with the relationship
81 between security awareness, our dependent variable, and each of the independent variables,
82 which include demographic variables, academic roles, familiarity with SSO, privacy concerns,
83 and Big-Five personality traits. Following that, we discuss the research design in detail,
84 including information about our participants, research instruments, and the data analysis
85 procedures. Finally, we present the statistical analysis results before discussing the key findings
86 and concluding by restating the main takeaways and identifying future research directions.

87

Theoretical Framework
Demographics and Security Awareness
90 Among demographic variables, gender and age have been identified as significant factors that
91 differentiate cyber security behaviors among users. For example, Anwar et al (2017) discovered
92 that female users are more likely than male users to have behaviors that increase the likelihood of
93 becoming a victim of cybercrimes. For example, they tend to reuse the same passwords across
94 multiple social media accounts, open email attachments from unknown people, and click peculiar
95 short URLs posted on the Internet. Meanwhile, Grimes et al (2010) discovered that older users
96 are less familiar with cyber security measures (e.g., keeping their passwords private) and are less
97 knowledgeable about cyber security risks (e.g., having difficulty in recognizing phishings,
98 computer viruses, and spams). In another study, Pratama & Firmansyah (2021) revealed that
99 females and older users were less likely to be aware of, let alone adopt, two-factor authentication
100 (2FA), making them particularly vulnerable to cyber security threats. Taking these findings into
101 account, we hypothesize that:
102
103   H1: Females are less aware of SSO security
104   H2: Older people are less aware of SSO security
105
106 It is worth highlighting that by no means do we assume that being female and older in and of
107 itself then make people less aware of SSO security. Rather, in this study we examine whether
108 such associations, which does not necessarily mean causation, as shown in the literature between
109 the respected demographic variables and security awareness still exist and if they are also true in
110 the case of SSO security. Such significant findings will expose demographic gaps needing to be
111 addressed by future research, for instance, on why the gaps keep occurring and how to close
112 them.

113

Academic Roles and Security Awareness

115 Most studies in cybersecurity awareness and behaviors in the academic community tend to focus
116 on either students (Farooq et al., 2015; Ngoqo & Flowerday, 2015; Zwilling et al., 2022) or
117 faculty/staff (Yerby & Floyd, 2018) only. In one study involving both academic roles,
118 faculty/staff reported higher security behaviors than students (Gratian et al., 2018). Taking that
119 into account and due to the nature of the role that faculty and staff usually have more systems
120 and data to access within an academic institution, and thus more to lose than students should
121 their SSO accounts be compromised, we hypothesize that:

123   H3: Students are less aware of SSO security than faculty and staff

SSO Familiarity and Security Awareness

126 SSO adoption in higher education is relatively recent in comparison to other industrial and
127 commercial organizations. In this particular institution where the study was conducted, the SSO
128 system, managed and operated directly by the university's Board of Information Systems, was
129 implemented using Shibboleth, an open source SSO system based on Security Assertion Markup
130 Language (SAML) protocol. The SSO was not fully implemented university-wide until 2019,
131 just a few months before the onset of the COVID-19 pandemic. Taking that into account, we
132 hypothesize that:

134   H4: Familiarity to SSO positively predicts SSO security awareness

Privacy Concerns and Security Awareness

137 Individual concerns over what, when, and how their private information is being shared to others
138 when using information technology products and services have been widely discussed in the
139 literature (Petronio & Child, 2020). For instance, multiple studies have revealed that the privacy
140 paradox, discrepancy between stated privacy attitudes and actual privacy behaviors, in using the
141 technologies does exist in various contexts and across cultures (Aleisa et al., 2020; Barth et al.,
142 2019; Kokolakis, 2017). Some argue that this phenomenon can be explained by privacy calculus,
143 which reflects the discrepancy between anticipated risks and expected benefits associated with
144 letting go of some private information (Goad et al., 2021). Should the benefits be higher, users
145 tend to compromise their privacy as opposed to holding it in any other cases. These arguments
146 suggest that privacy concerns lead to more cautious decisions in whether to use information
147 technology related products or services, including SSO implementation as pointed out by some
148 studies in the literature (Cho et al., 2020; Heckle & Lutters, 2007). Bringing all those findings to
149 the current study's context, we predict that:

151   H5: Privacy concerns positively predict SSO security awareness

Big-Five Personality and Security Awareness

154 Earlier psychological research established a link between cyber security behavior and the Big-
155 Five personality, the characteristics of which are summarized in Table 1 (Gosling et al., 2003).
156 For instance, Russell et al (2017) found negative correlations between emotional instability
157 (neuroticism) and secure cyber behaviors (e.g., using protection software against malware and
158 virus) and between conscientiousness and insecure cyber behaviors (e.g., using unsecured
159 wireless networks), whereas Shappie et al (2020) revealed that in addition to conscientiousness;
160 agreeableness and openness positively predict cybersecurity behaviors (e.g., keeping anti-virus
161 software up to date). Meanwhile, Kennison & Chan-Tin (2020) reported rather different results:
162 extraversion, agreeableness, and emotional stability -not openness nor conscientiousness- explain
163 why some users are prone to commit risky cyber behaviors (e.g., not signing out of a shared
164 computer, sharing password with someone else) while others are not.

165 It appears that the relationships between Big-Five personality traits and cybersecurity awareness
166 seem to vary across contexts and depend on the indicators measured in the study. However, in
167 terms of SSO security awareness, and also by taking into consideration the Indonesian context as
168 a collectivist country, we argue that being extraverted and agreeable is associated with lower
169 SSO security awareness. Users having these traits are more likely to share their passwords with
170 someone else, either voluntarily out of trust or when asked by others they respect or fear due to
171 social status. On the other hand, we argue that being conscientious, emotionally stable, and open
172 is associated with higher SSO security awareness. Users having these traits are arguably more
173 cautious in their decision making and thus will avoid risky behavior with their SSO accounts.
174 Thus, our hypotheses are as follows:

175
176   H6: Extraversion negatively predicts SSO awareness
177   H7: Agreeableness negatively predicts SSO awareness
178   H8: Conscientiousness positively predicts SSO awareness
179   H9: Emotional stability positively predicts SSO awareness
180   H10: Openness positively predicts SSO awareness

181
182 Furthermore, since past studies reported significant correlations between agreeableness and
183 privacy concerns (Korzaan & Boswell, 2008), and between conscientiousness and privacy
184 concerns (Junglas et al., 2008), we thus expect the aforementioned variables will interact with
185 each other in predicting SSO security awareness. As such, our two final hypotheses are as
186 follows:

187
188   H11: Agreeableness interacts with privacy concerns in predicting SSO security awareness
189   H12: Conscientiousness interacts with privacy concerns in predicting SSO security
190   awareness

191
192 **Materials & Methods**

193 **Participants**
194 After obtaining approval from the Directorate of Research and Community Services within the
195 university (No: 01.A/DirDPPM/70/DPPM/I/2021), we sent out a link to an online survey through
196 broadcast email and WhatsApp messages to the academic community at one of the largest
197 private universities in Indonesia, which has approximately 23,000 students and 1,000 faculty and
198 staff. Between April 16 and May 4, 2021, a total of 283 participants ranging from 17 to 59 years
199 of age (M = 26.63, SD = 10.23) completed the survey after providing their consents. The
200 questionnaire was delivered in Bahasa Indonesia (see Supplementary Materials). To ensure
201 eligibility and avoid duplication, all participants were required to use their SSO accounts to
202 access the survey. More information about the demographics of respondents is available in Table
203 2.
204
205 **Measures**
206 Apart from the three demographic variables (i.e., gender, age, and academic role), there are three
207 independent variables (i.e., SSO familiarity, privacy concerns, and Big-Five personality) and
208 one dependent variable (SSO account security awareness) in this study. Table 3 summarizes the
209 variables of interest along with their respective measurement items that we developed for this
210 study as follows:
211
212 *SSO Familiarity.* We developed three items to measure how well users are familiar with the SSO
213 system in their university. The three items cover their overall knowledge of SSO along with its
214 features and risk. We then aggregated the three items to calculate a composite score of SSO
215 familiarity in the range of 0 to 100.
216
217 *Privacy Concerns.* We adopted privacy concerns scales developed by Buchanan et al (2007) to
218 measure user privacy concerns in this study. Specifically, we included only five items related to
219 user accounts. We also calculated a composite score of privacy concerns in the range of 0 to 100
220 by aggregating all five items.
221
222 *Big-Five Personality.* We adopted the Ten Item Personality Inventory (TIPI), a very brief
223 measure of the Big-Five personality domains (Gosling et al., 2003), which has been widely used
224 by many researchers in need of short personality measures in the past two decades. Specifically,
225 we used the one that has been translated and validated in Bahasa Indonesia (Hanif, 2018) in this
226 study.
227
228 *SSO Account Security Awareness.* We developed five items for each one of the Knowledge,
229 Attitude, and Behavior dimension, resulting in a total of 15 items to measure SSO Account
230 Security Awareness in this study by adapting the Human Aspects of the Information Security
231 Questionnaire (HAIS-Q) (Parsons et al., 2017). We then calculated a composite score of SSO
232 account security awareness in the range of 0 to 100 by using the weighted average method (30%
233 for Knowledge, 20% for Attitude, and 50% for Behavior) to be classified further into three

234 categories, i.e., "Poor" (< 60), "Average" (60-79.99), and "Good" (≥ 80) as recommended by
235 Kruger & Kearney (2006).

236

237 **Data Analysis**
238 We employed hierarchical linear regression in R 3.6.3 to analyze the data. As illustrated in
239 Figure 1, we conducted three steps of regression analysis with some additional independent
240 variables in each model. In the first regression, we included only SSO familiarity and privacy
241 concerns in addition to the three demographic variables (i.e., gender, age, and academic role) as
242 the predictors. Next, we introduced the Big-Five personality variables to the model in the second
243 regression. Finally, we added the interaction terms between privacy concerns and two out of five
244 Big-Five personality variables (i.e., agreeableness and conscientiousness) in the third regression
245 following the link between them as shown in the literature (Osatuyi, 2015). Additionally, we ran
246 several diagnostic tests on the regression model (i.e., Residual Plot, Normal Q-Q Plot, Scale-
247 Location Plot, and Cook's distance) to look for potential outliers where we identified three
248 influential cases that we then omitted prior to repeating the hierarchical regression analysis. The
249 dataset along with the corresponding R code for analysis are available on our GitHub repository[1].

250

251 # Results
252 The summary statistics are provided in Table 4 for the dependent variable and in Table 5 for the
253 independent variables. As can be seen, the average SSO security awareness score for all
254 participants in this study is 69.31 out of 100, which falls into the "Average" category according
255 to the rubric by Kruger & Kearney (2006). When considering each individual measurement item,
256 the mean for the majority of items is indeed between 60 and 79.99. Certain items relating to
257 password reuse (K1, A1), password length (K4, A4), and the use of incognito mode on a shared
258 device (B5) are classified as "Poor", while others relating to account sharing (K2, A2, B2) and
259 password complexity (K3) are classified as "Good". Applying the same categorization to SSO
260 familiarity (i.e., 80.86 out of 100) and privacy concerns (i.e., 85.90 out of 100), however, means
261 they both fall into the "Good" category.

262 The scatterplots in Figure 2 illustrate how SSO security scores vary by demographic variables.
263 As can be seen, the SSO security awareness scores and age tend to form a negative linear
264 relationship. This relationship is typically consistent across genders and academic roles.

265 Additionally, the dumbbell plots in Figure 3 indicate that SSO security awareness is relatively
266 consistent across genders, but not across academic roles. Students consistently demonstrated
267 significantly lower levels of knowledge, attitude, and behavior regarding SSO account security
268 compared to faculty and staff. Apart from their score in attitude that is much lower and closer to
269 student's score, staff scored fairly close to faculty in terms of knowledge and behavior, resulting
270 in no significant differences in total score between the two.

---

[1] https://github.com/ahmadrafie/ssostudy

271   Following that, Table 6 summarizes the results of the hierarchical regression analysis. As can be
272   seen, all independent variables, with the exception of gender, were found to be statistically
273   significant in the first regression and they remained significant in the second regression after the
274   addition of Big-Five personality traits as independent variables in the model. While only one of
275   the five personality traits (i.e., extraversion) was found to be statistically significant in the second
276   regression, the addition of interaction terms between some traits (i.e., agreeableness and
277   conscientiousness) and privacy concerns in the third regression altered the result. As it turned
278   out, statistical significance was found for all but one of the Big-Five personality traits (i.e.,
279   openness). With the addition of these interaction terms, another significant finding emerged:
280   privacy concerns were no longer significant predictors of SSO security awareness on their own.
281   Rather than that, they interact with agreeableness and conscientiousness, as depicted in Figure 4.
282   Furthermore, as shown in Table 6, these interaction terms are the two strongest predictors in the
283   final model based on their standardized coefficients.

284   Taking all of the preceding findings into account, Table 7 summarizes the results of hypothesis
285   tests and Figure 5 illustrates the final model based on those findings.
286

Discussion

288   **Demographics and SSO Security Awareness**
289   As illustrated in Figure 2 and futher confirmed in Table 6, the generational gap remains present
290   in this study. Older users have lower security awareness than their younger colleagues. While
291   arguments from prior research that older people did not get the same chance as younger people
292   did in terms of digital literacy exposure including cyber security measures (Grimes et al., 2010)
293   may still hold water, this finding brings a more serious issue in this study's context. In Indonesia,
294   which may also be true in many other countries, age arguably correlates with job seniority
295   position. Putting this into the context of SSO, therefore, the older the users, the more systems and
296   information are at risk should any cybersecurity incidents happen. Linking with our previous
297   argument that users of the same educational setting should arguably receive similar exposure, it
298   could be the case that such programs used by the IT department in introducing SSO technology
299   and its security may not well address their older users yet. In other words, they seem to work
300   effectively only for younger generations. The fact that SSO familiarity significantly predicts SSO
301   awareness further supports our argument.

302   Interestingly, our analysis results confirmed all demographic hypotheses except for gender. As
303   illustrated in Figure 3, the security awareness scores are nearly identical between males and
304   females. Even more so, the association between gender and SSO security awareness remains
305   non-significant after putting psychological factors as well as their interaction terms with privacy
306   concerns into the equation as shown in Table 6. These unexpected findings contradict past
307   research reporting that female users tend to be less aware of cyber security measures (Anwar et
308   al., 2017; Pratama & Firmansyah, 2021). Considering that this study takes place within a single
309   higher education institution, it could be the case that both male and female users have already

310   been exposed to similar levels of SSO usage within their institution. Ergo, such gender
311   distinctions have no bearing on their security awareness. The absence of statistically significant
312   differences in SSO security awareness between males and females in this study is encouraging
313   because it demonstrates that organizations can rely on both male and female users having the
314   same level of SSO security awareness. It could also be attributed to the organization's success in
315   educating users regardless of their gender.

316   On the other hand, past research indicating gender gap in cybersecurity awareness either took
317   place in a workplace in which participants' chances to get exposed to such cyber measures might
318   vary (Anwar et al., 2017) or their participants came from different places altogether (Pratama &
319   Firmansyah, 2021). Those having IT related backgrounds and working directly with external
320   clients might be more aware of cyber threats compared to those having no IT backgrounds and
321   working with internal clients only. Considering that females are still underrepresented in IT
322   related jobs (Richter, 2021), it could be the main reason why such a gender gap existed in past
323   research. As such, we argue that any study revealing a gender disparity in cybersecurity
324   awareness should delve deeper into the reason for it than simply gender.

325   As also illustrated in Figure 3 and confirmed in Table 6, we found that students are less aware of
326   SSO security than staff and faculty, who share similar SSO security awareness level. On one
327   hand, it can be the case because they have less things to lose if such incidents happen. As
328   Pratama & Firmansyah, (2021) argue, how sensitive people are to cyber threats and how well
329   they adhere to cyber security measures is directly proportional to the magnitude of their potential
330   losses should such incidents occur. Students, arguably, have less to lose in regard to their SSO
331   account. On the contrary, faculty and academic staff have a plethora of sensitive data at risk,
332   ranging from financial and salary information to any other private or confidential data, both to
333   them as users and to their institution. As such, it is unsurprising that faculty and staff are more
334   cognizant of SSO account security than students are. On the other hand, the fact that students are
335   significantly less aware of SSO account security also leads to another suspicious behavior. Some
336   students might intentionally share their SSO accounts. While it would be unethical to suspect all
337   students, given that academic cheating is perceived as collaboration in collectivistic cultures such
338   as Indonesia (Jamaluddin et al., 2021), the possibility that a few students misuse their SSO
339   accounts by intentionally sharing them with each other for academic dishonesty cannot be ruled
340   out.

341

342   **Privacy Concerns, Big-Five Personality, and SSO Security Awareness**
343   As expected, privacy concerns are positively associated with SSO security awareness, at least in
344   the first two regressions as shown in Table 6. Holding all other variables constant, the more
345   concerned users are about their privacy, the more aware they are of SSO security. Interestingly,
346   when we factor in their interaction with the Big-Five personality constructs, this association
347   becomes irrelevant. In other words, the extent to which privacy concerns may affect users' SSO
348   security awareness is determined by their personality traits. Users with a high degree of

349 agreeableness (i.e., warm, not critical) are generally less aware of SSO security, but this would
350 change if they also had increased privacy concerns. On the contrary, users who are naturally
351 conscientious (i.e., organized, cautious) tend to have a high level of security awareness regarding
352 their SSO accounts regardless of their privacy concerns, even if the latter can help those with a
353 low degree of conscientiousness improve their security awareness. In this regard, regardless of
354 their level of privacy concerns, it is the users' personality that naturally compels them to be more
355 circumspect and critical, thereby increasing their awareness of the risks associated with their
356 SSO accounts.

357 In contrast to the two aforementioned traits, extraversion and emotional stability account for SSO
358 security awareness in ways that go beyond privacy concerns. In this regard, the more extraverted
359 users are, the less aware they are of SSO security. By contrast, users who are emotionally stable
360 are more likely to be aware of SSO security. Interestingly, even after controlling for
361 demographic and privacy concerns variables, only the openness trait has no significant
362 association with SSO security awareness. Our attempt to determine whether there are any
363 interactions between these three characteristics and privacy concerns, which revealed none,
364 confirms that these findings are robust.

365 These findings altogether suggest the needs of a tailored approach should interventions be
366 designed to increase users' SSO security awareness. For example, intervention emphasizing
367 privacy risk may work best for users with a high degree of agreeableness but is less efficient for
368 users with high degree of conscientiousness. While for users with a high degree of emotional
369 stability, it may be better to teach them about SSO security measures. A particular attention
370 should be paid to users with extraverted traits given the negative association with security
371 awareness in the model. Some conventional interventions may not work as effectively as it is for
372 other personality traits. Perhaps, such further behavioral interventions may be needed. We
373 suggest future research to explore this area more to shed light on different types of education and
374 interventions that can work better for different types of personality traits.

375

376 ## Conclusions
377 Our study discovered unique relationships between SSO security awareness, demographic
378 characteristics, privacy concerns, and personality traits. The degree to which users are aware of
379 SSO security varies according to their demographic characteristics and is determined in part by
380 their personality traits, some of which (i.e., agreeableness and conscientiousness) interact with
381 their level of privacy concerns. The absence of gender disparities in SSO security awareness in
382 this study suggests that it is possible to close the gap under the right circumstances, including but
383 not limited to education and policy. It also suggests that closing generational gaps may be a
384 greater challenge than closing gender gaps in cybersecurity awareness.

385 **Future Work**

386   This study lays the groundwork for future research and interventions aimed at increasing user
387   awareness of SSO security and closing any existing gaps between different demographic groups
388   of users, particularly in higher education settings. An experimental study examining various
389   types of intervention on SSO security awareness is one way to accomplish this. With the growing
390   adoption of SSO by colleges and universities worldwide, addressing this issue of SSO security
391   awareness is becoming increasingly important. Also, to gain a more holistic understanding of
392   security awareness and practices surrounding SSO, we propose that researchers conduct similar
393   studies in other parts of the world, taking into account cultural differences that may affect
394   cybersecurity awareness, particularly regarding SSO security.

395

Acknowledgements

397   We would like to express our gratitude to Dr. Mukhammad Andri Setiawan and his team at the
398   Board of Information Systems for providing technical information about the university's SSO
399   implementation, and to the Division of Public Relations for assisting us with data collection.

400

References

402   Aleisa, N., Renaud, K., & Bongiovanni, I. (2020). The privacy paradox applies to IoT devices
403   too: A Saudi Arabian study. *Computers & Security*, *96*, 101897.
404   https://doi.org/10.1016/j.cose.2020.101897
405   Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and
406   employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443.
407   https://doi.org/10.1016/j.chb.2016.12.040
408   Bai, G., Lei, J., Meng, G., Venkatraman, S. S., Saxena, P., Sun, J., Liu, Y., & Dong, J. S. (2013).
409   *AUTHSCAN: Automatic extraction of web authentication protocols from implementations*.
410   1. https://ink.library.smu.edu.sg/sis_research/5008/
411   Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the
412   privacy paradox to the test: Online privacy and security behaviors among users with
413   technical knowledge, privacy awareness, and financial resources. *Telematics and*
414   *Informatics*, *41*, 55–69. https://doi.org/10.1016/j.tele.2019.03.003
415   Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of
416   online privacy concern and protection for use on the Internet. *Journal of the American*
417   *Society for Information Science and Technology*, *58*(2), 157–165.
418   https://doi.org/10.1002/asi.20459
419   Chinitz, J. (2000). Single Sign-On: Is It Really Possible? *Information Systems Security*, *9*(3), 1–
420   14. https://doi.org/10.1201/1086/43310.9.3.20000708/31359.5
421   Cho, E., Kim, J., & Sundar, S. S. (2020). Will You Log into Tinder using your Facebook
422   Account? Adoption of Single Sign-On for Privacy-Sensitive Apps. *Extended Abstracts of*
423   *the 2020 CHI Conference on Human Factors in Computing Systems*, 1–7.
424   https://doi.org/10.1145/3334480.3383074

425 Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information Security Awareness in
426   Educational Institution: An Analysis of Students' Individual Factors. In *2015 IEEE*
427   *Trustcom/BigDataSE/ISPA*. https://doi.org/10.1109/trustcom.2015.394
428 Gellert, G., Crouch, J. F., Gibson, L. A., & Conklin, G. S. (2019). An Evaluation of the Clinical
429   and Financial Value of Work Station Single Sign-on in 19 Hospitals. *Perspectives in Health*
430   *Information Management / AHIMA, American Health Information Management*
431   *Association*, *16*(Summer), 1a. https://www.ncbi.nlm.nih.gov/pubmed/31423117
432 Goad, D., Collins, A. T., & Gal, U. (2021). Privacy and the Internet of Things−An experiment in
433   discrete choice. *Information & Management*, *58*(2), 103292.
434   https://doi.org/10.1016/j.im.2020.103292
435 Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big-Five
436   personality domains. *Journal of Research in Personality*, *37*(6), 504–528.
437   https://doi.org/10.1016/S0092-6566(03)00046-1
438 Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits
439   and cyber security behavior intentions. *Computers & Security*, *73*, 345–358.
440   https://doi.org/10.1016/j.cose.2017.11.015
441 Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older Adults' Knowledge
442   of Internet Hazards. *Educational Gerontology*, *36*(3), 173–192.
443   https://doi.org/10.1080/03601270903183065
444 Hanif, A. (2018). Translation and validation of the Ten-Item Personality Inventory (TIPI) into
445   Bahasa Indonesia. *International Journal of Research*, *7*(2), 59–69.
446   https://gosling.psy.utexas.edu/wp-content/uploads/2018/05/TIPI-Indonesia_MS.pdf
447 Heckle, R. R., & Lutters, W. G. (2007). Privacy implications for single sign-on authentication in
448   a hospital environment. *Proceedings of the 3rd Symposium on Usable Privacy and Security*,
449   173–174. https://doi.org/10.1145/1280680.1280714
450 Jamaluddin, S. F., Adi, S. P., & Lufityanto, G. (2021). Social influences on cheating in
451   collectivistic culture: Collaboration but not competition. *Group Dynamics: Theory,*
452   *Research, and Practice: The Official Journal of Division 49, Group Psychology and Group*
453   *Psychotherapy of the American Psychological Association*, *25*(2), 174–189.
454   https://doi.org/10.1037/gdn0000122
455 James, N., Marwaha, S., Brough, S., & John, T. T. (2020). Impact of Single Sign-on Adoption in
456   an Assessment Triage Unit: A Hospital's Journey to Higher Efficiency. *The Journal of*
457   *Nursing Administration*, *50*(3), 159–164. https://doi.org/10.1097/NNA.0000000000000860
458 Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for
459   privacy: an empirical study in the context of location-based services. *European Journal of*
460   *Information Systems*, *17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29
461 Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge
462   and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Frontiers in*
463   *Psychology*, *11*, 546546. https://doi.org/10.3389/fpsyg.2020.546546
464 Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on

465   the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

466   https://doi.org/10.1016/j.cose.2015.07.002

467   Korzaan, M. L., & Boswell, K. T. (2008). The Influence of Personality Traits and Information

468   Privacy Concerns on Behavioral Intentions. *Journal of Computer Information Systems*,

469   *48*(4), 15–24. https://doi.org/10.1080/08874417.2008.11646031

470   Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security

471   awareness. *Computers & Security*, *25*(4), 289–296.

472   https://doi.org/10.1016/j.cose.2006.02.008

473   Lane, M., & Marie, M. (2010). The adoption of single sign-on and multifactor authentication in

474   organisations-A critical evaluation using TOE framework. *Information in Motion*, *7*, 161.

475   Ngoqo, B., & Flowerday, S. V. (2015). Exploring the relationship between student mobile

476   information security awareness and behavioural intent. *Information & Computer Security*,

477   *23*(4), 406–420. https://doi.org/10.1108/ICS-10-2014-0072

478   Osatuyi, B. (2015). Personality Traits and Information Privacy Concern on Social Media

479   Platforms. *Journal of Computer Information Systems*, *55*(4), 11–19.

480   https://doi.org/10.1080/08874417.2015.11645782

481   Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The

482   Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation

483   studies. *Computers & Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

484   Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: utility of

485   communication privacy management theory. *Current Opinion in Psychology*, *31*, 76–82.

486   https://doi.org/10.1016/j.copsyc.2019.08.009

487   Pratama, A. R., & Firmansyah, F. M. (2021). Until you have something to lose! Loss aversion

488   and two-factor authentication adoption. *Applied Computing and Informatics*, *ahead-of-*

489   *print*(ahead-of-print). https://doi.org/10.1108/ACI-12-2020-0156

490   Richter, F. (2021). *Women's representation in big tech*. Statista Infographics.

491   https://www.statista.com/chart/4467/female-employees-at-tech-companies/ (Original work

492   published 2021)

493   Russell, J. D., Weems, C. F., Ahmed, I., & Richard, G. G., III. (2017). Self-reported secure and

494   insecure cyber behaviour: factor structure and associations with personality factors. *Journal*

495   *of Cyber Security Technology*, *1*(3-4), 163–174.

496   https://doi.org/10.1080/23742917.2017.1345271

497   Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity

498   behavior. *Psychology of Popular Media*, *9*(4), 475–480.

499   https://doi.org/10.1037/ppm0000247

500   Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2011). What

501   makes users refuse web single sign-on? an empirical investigation of OpenID. *Proceedings*

502   *of the Seventh Symposium on Usable Privacy and Security*, 1–20.

503   https://doi.org/10.1145/2078827.2078833

504   Yerby, J., & Floyd, K. (2018). Faculty and Staff Information Security Awareness and Behaviors.

505   *Journal of The Colloquium for Information Systems Security Education*, *6*(1), 23–23.

506   https://cisse.info/journal/index.php/cisse/article/view/90

507   Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber

508   Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer*

509   *Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Big-Five Personality

1   Table 1 Big-Five Personality

Personality	Traits
Extraversion	Enthusiastic, not reserved, extraverted, not quiet
Agreeableness	Not critical, sympathetic, warm, not quarrelsome
Conscientiousness	Organized, careful, dependable, self-disciplined
Emotional stability	Not anxious, not easily upset, calm, emotionally stable
Openness	Creative, not conventional, open to new experience, complex

Demographic information of all participants (n=283)

1   Table 2. Demographic information of all participants (n=283)

Variable	Frequency	Percentage
Gender		
Male	148	52%
Female	135	48%
Age		
≤ 19 years old	72	25%
20-29 years old	132	47%
30-39 years old	38	13%
40-49 years old	31	11%
≥ 50 years old	10	4%
Academic Role		
Student	197	70%
Faculty member	34	12%
Staff	52	18%

Variables of interest and measurement items

* reverse items were inverted prior to calculation

1   Table 3. Variables of interest and measurement items

Variable	Code
Familiarity with SSO	**F**
1. I know what the university's SSO account is.	F1
2. I know what systems and data are accessible with my university's SSO account.	F2
3. I am aware of the risk of negative impacts if my university's SSO account is used by other people.	F3
Privacy concerns	**Pr**
1. In general, how concerned are you about your privacy while you are using the internet?	Pr1
2. Are you concerned about online organizations not being who they claim they are?	Pr2
3. Are you concerned about online identity theft?	Pr3
4. Are you concerned about people online not being who they say they are?	Pr4
5. Are you concerned that an email you send may be read by someone else besides the person you sent it to?	Pr5
Knowledge	**K**
1. Using the same password for the university's SSO account and other personal accounts like social media is not prohibited.	K1r*
2. Sharing my password for the university's SSO account to other people, including friends or colleagues, is not prohibited.	K2r*
3. A combination of uppercase, lowercase, numbers, and special characters is a must when choosing password, including for the university's SSO account.	K3
4. Using a password that is 8 characters long or shorter is not prohibited.	K4r*
5. When signing-in to the university account through the SSO system on a device that is not my own, using the incognito or private mode in the web browser is necessary.	K5
Attitude	**A**
1. It is safe enough to use the same password for the university's SSO account and other personal accounts like social media.	A1r*
2. Sharing my password for the university's SSO account to other people, including friends or colleagues, is a bad idea.	A2
3. It is safe enough to use a password that consists of a combination of only alphabets, including for the university's SSO account.	A3r*
4. It is safe enough to use a password that is 8 characters long or shorter, including for the university's SSO account.	A4r*
5. Signing into the university's SSO account on a device that is not my own without using the incognito or private mode in the web browser is risky.	A5
Behavior	**B**
1. I use a different password for the university's SSO account than my other	B1

personal accounts like social media.

2. I share my password for the university's SSO account with friends or colleagues at the university.   B2r*

3. I use a combination of uppercase, lowercase, numbers, and special characters for all my passwords, including the university's SSO account.   B3

4. I always use passwords that are more than 8 characters long, including for the university's SSO account.   B4

5. I hardly ever use incognito or private mode in the web browser when signing into the university's SSO account on a device that is not my own.   B5r*

Security Awareness Score	**Score**

Note: * reverse items were inverted prior to calculation

Summary statistics of the dependent variable

Table 4. Summary statistics of the dependent variable

Variable	Mean	SD	Min	Max
Knowledge (0-100)	**66.91**	**16.26**	**25**	**100**
K1: password reuse	47.00	34.59	0	100
K2: sharing SSO account	82.86	26.00	0	100
K3: password complexity	84.28	25.18	0	100
K4: password length	46.38	33.32	0	100
K5: incognito mode	74.03	26.07	0	100
Attitude (0-100)	**62.69**	**18.90**	**15**	**100**
A1: password reuse	51.50	33.32	0	100
A2: sharing SSO account	80.83	28.97	0	100
A3: password complexity	60.51	30.11	0	100
A4: password length	42.84	31.29	0	100
A5: incognito mode	77.74	24.35	0	100
Behavior (0-100)	**73.41**	**14.96**	**25**	**100**
B1: password reuse	77.56	27.37	0	100
B2: sharing SSO account	86.31	23.45	0	100
B3: password complexity	78.45	24.72	0	100
B4: password length	75.00	26.46	0	100
B5: incognito mode	49.73	31.54	0	100
Composite Score (0-100)	**69.31**	**13.62**	**34.5**	**100**

Summary statistics of the independent variables

1 Table 5. Summary statistics of the independent variables

Variable	Mean	SD	Min	Max
Familiarity with SSO (0-100)	**80.86**	**18.56**	**25**	**100**
F1: know what SSO is	82.60	20.19	0	100
F2: know what systems and data are accessible with SSO	77.12	23.06	0	100
F3: aware of the risk of SSO account being used by others	82.86	23.40	0	100
Privacy Concerns (0-100)	**85.90**	**14.54**	**30**	**100**
P1: general privacy concerns on the Internet	79.95	20.46	0	100
P2: false identity of organizations online	84.72	20.59	0	100
P3: online identity theft	84.28	20.20	0	100
P4: false identity of other individuals online	93.11	14.78	0	100
P5: confidentiality of messages	87.46	19.57	0	100
Big-Five Personality (1-7)				
Extraversion	4.14	1.18	1.00	7.00
Agreeableness	5.30	1.03	1.00	7.00
Conscientiousness	5.14	1.05	2.50	7.00
Emotional Stability	4.71	1.20	2.00	7.00
Openness	5.33	1.07	1.50	7.00

Hierarchical regression analysis

* Faculty member is used as the reference category; numbers reported are unstandardized coefficients (B), standard errors of unstandardized coefficients (SE B), standardized coefficients (β), and p-values (*p*); the bold and blue numbers denote statistically significant values (p < .05);

1   Table 6. Hierarchical regression analysis

Predictor Variables	Regression 1				Regression 2				Regression 3			
	B	SE B	β	*p*	B	SE B	β	*p*	B	SE B	β	*p*
Constant	63.37	8.68	-	<.001	67.83	9.49	-	<.001	71.46	25.67	-	.006
Gender (Male)	-0.14	1.55	-0.01	.931	-0.77	1.57	-0.03	.625	-0.82	1.54	-0.03	.592
Age	**-0.36**	**0.14**	**-0.28**	**.010**	**-0.34**	**0.14**	**-0.26**	**.013**	**-0.35**	**0.14**	**-0.27**	**.011**
Academic Role *												
- Staff	-2.40	2.80	-0.07	.391	-2.77	2.77	-0.08	.317	-2.87	2.73	-0.08	.294
- Student	**-13.79**	**3.50**	**-0.48**	**<.001**	**-12.88**	**3.46**	**-0.45**	**<.001**	**-13.25**	**3.42**	**-0.46**	**<.001**
Familiarity with SSO Account	**0.11**	**0.04**	**0.16**	**.007**	**0.10**	**0.04**	**0.14**	**.023**	**0.10**	**0.04**	**0.14**	**.024**
Privacy concerns	**0.15**	**0.06**	**0.17**	**.007**	**0.15**	**0.06**	**0.16**	**.010**	0.11	0.29	-0.12	.692
Big-Five Personality												
- Extraversion					**-1.47**	**0.66**	**-0.13**	**.027**	**-1.31**	**0.65**	**-0.12**	**.046**
- Agreeableness					-0.93	0.86	-0.07	.282	**-16.11**	**5.04**	**-1.22**	**.002**
- Conscientiousness					1.57	0.87	0.12	.074	**15.43**	**5.41**	**1.21**	**.005**
- Emotional Stability					1.37	0.79	0.12	.085	**1.63**	**0.79**	**0.15**	**.038**
- Openness					-0.73	0.83	-0.06	.385	-0.73	0.82	-0.06	.378
Interaction Terms												
- Privacy concerns x Agreeableness									**0.17**	**0.06**	**1.56**	**.003**
- Privacy concerns x Conscientiousness									**-0.16**	**0.06**	**-1.42**	**.011**
Observations	280				280				280			
df	273				268				266			
p	<.001				<.001				<.001			
R²	0.125				0.170				0.201			

	0.106	0.136	0.162
Adjusted R^2	0.106	0.136	0.162
ΔR^2	-	0.045	0.031
ΔAdjusted R^2	-	0.030	0.026

2 **Note:** * Faculty member is used as the reference category; numbers reported are unstandardized coefficients (B), standard errors of
3 unstandardized coefficients (SE B), standardized coefficients (β), and p-values (p); the bold and blue numbers denote statistically
4 significant values (p < .05);

Summary of hypothesis tests results

1 Table 7. Summary of hypothesis tests results

Hypothesis	Relationship	Result
H1	Females are less aware of SSO security	Not supported
H2	Older people are less aware of SSO security	Supported
H3	Students are less aware of SSO security than faculty/staff	Supported
H4	Familiarity to SSO positively predicts SSO security awareness	Supported
H5	Privacy concerns positively predict SSO security awareness	Partially supported
H6		Supported
H7	Extraversion negatively predicts SSO awareness	Supported
H8	Agreeableness negatively predicts SSO awareness	Supported
H9	Conscientiousness positively predicts SSO awareness	Supported
H10	Emotional stability positively predicts SSO awareness	Not supported
H11	Openness positively predicts SSO awareness	Supported
	Agreeableness interacts with privacy concerns in predicting	
H12	SSO security awareness	Supported
	Conscientiousness interacts with privacy concerns in predicting SSO security awareness	

Figure 1

Conceptual model of SSO account security awareness in this study
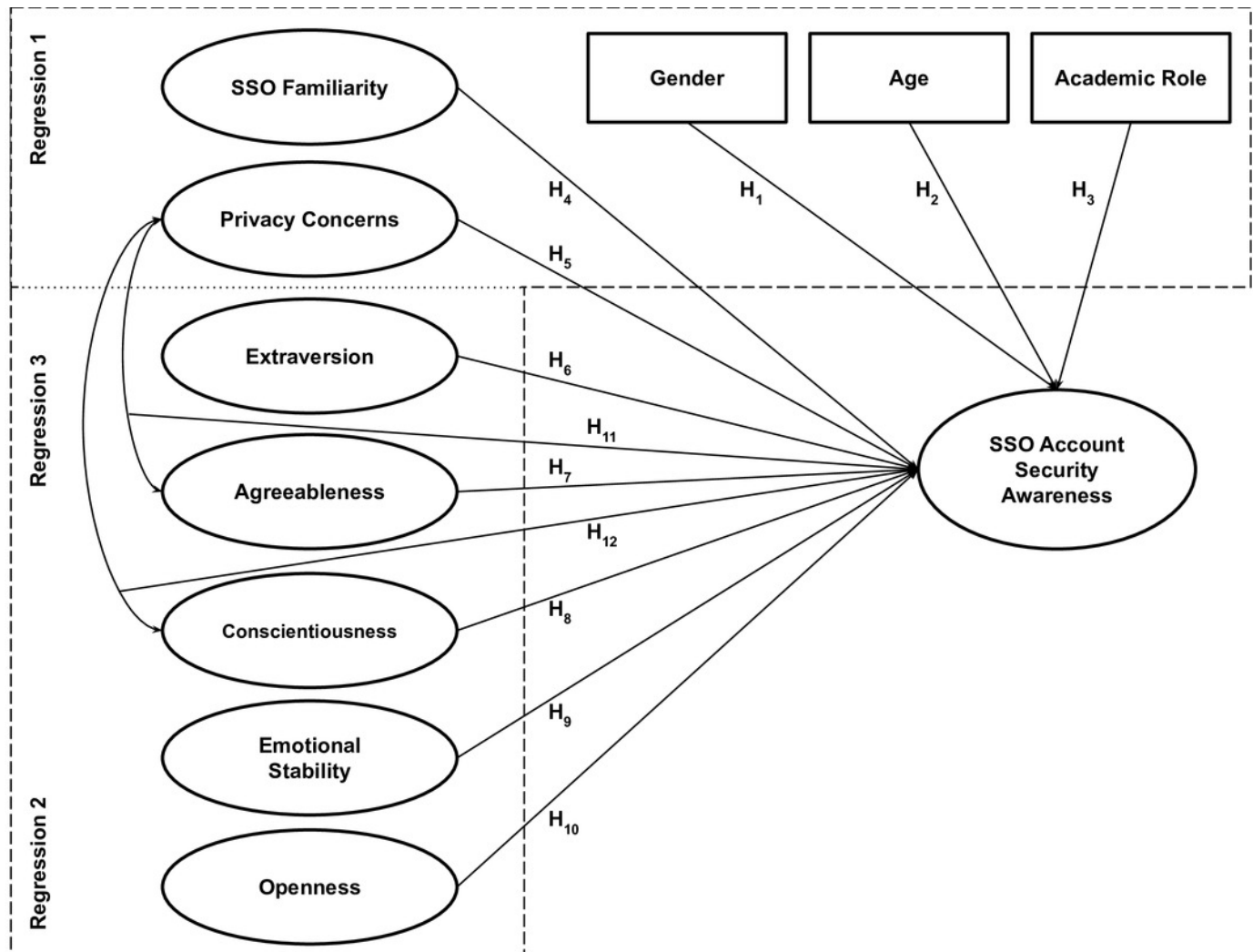
Figure 2

Scatterplots of SSO security awareness score by age, gender, and academic roles
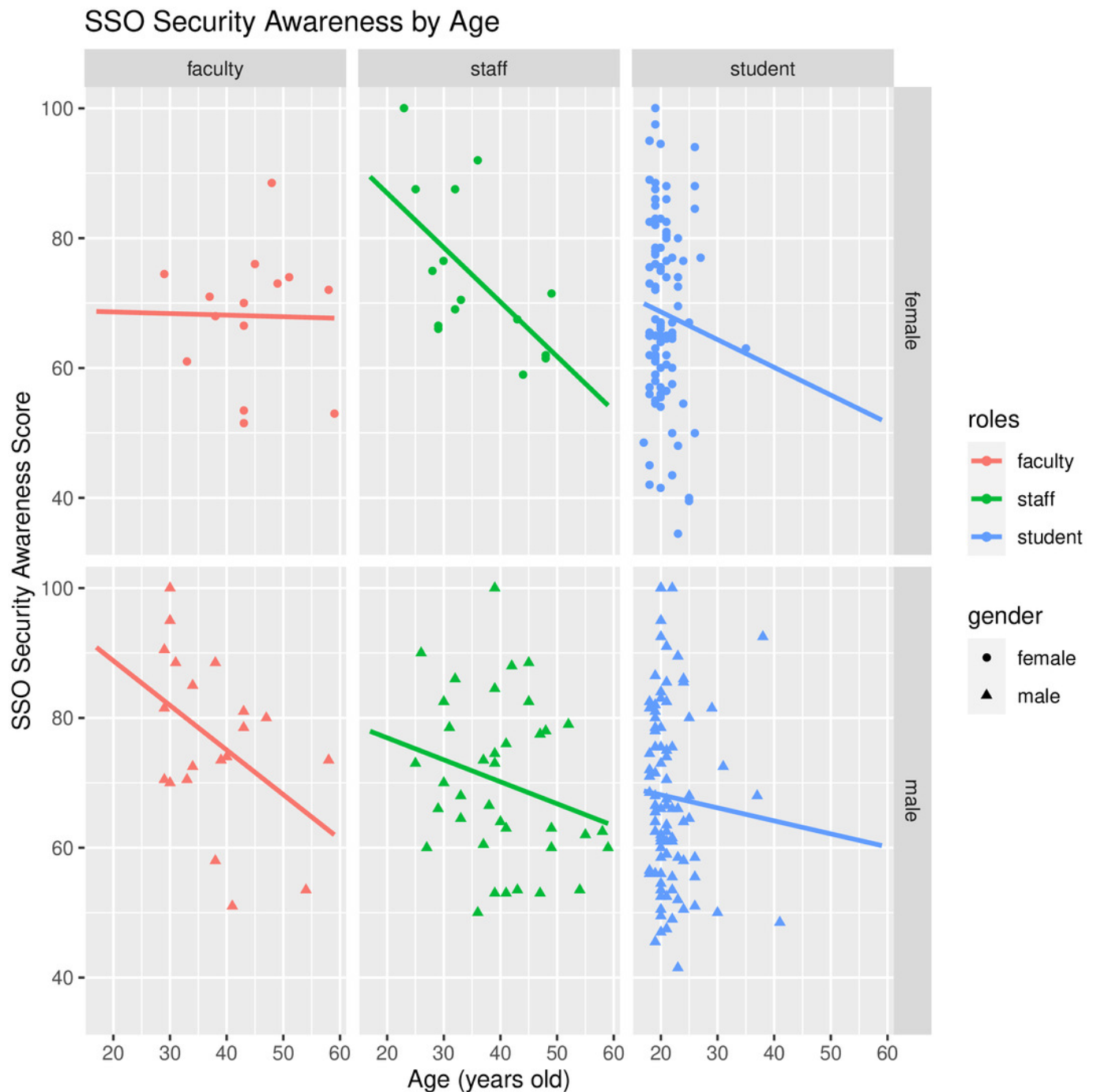
Figure 3

Dumbbell plots of SSO security awareness by gender and academic roles
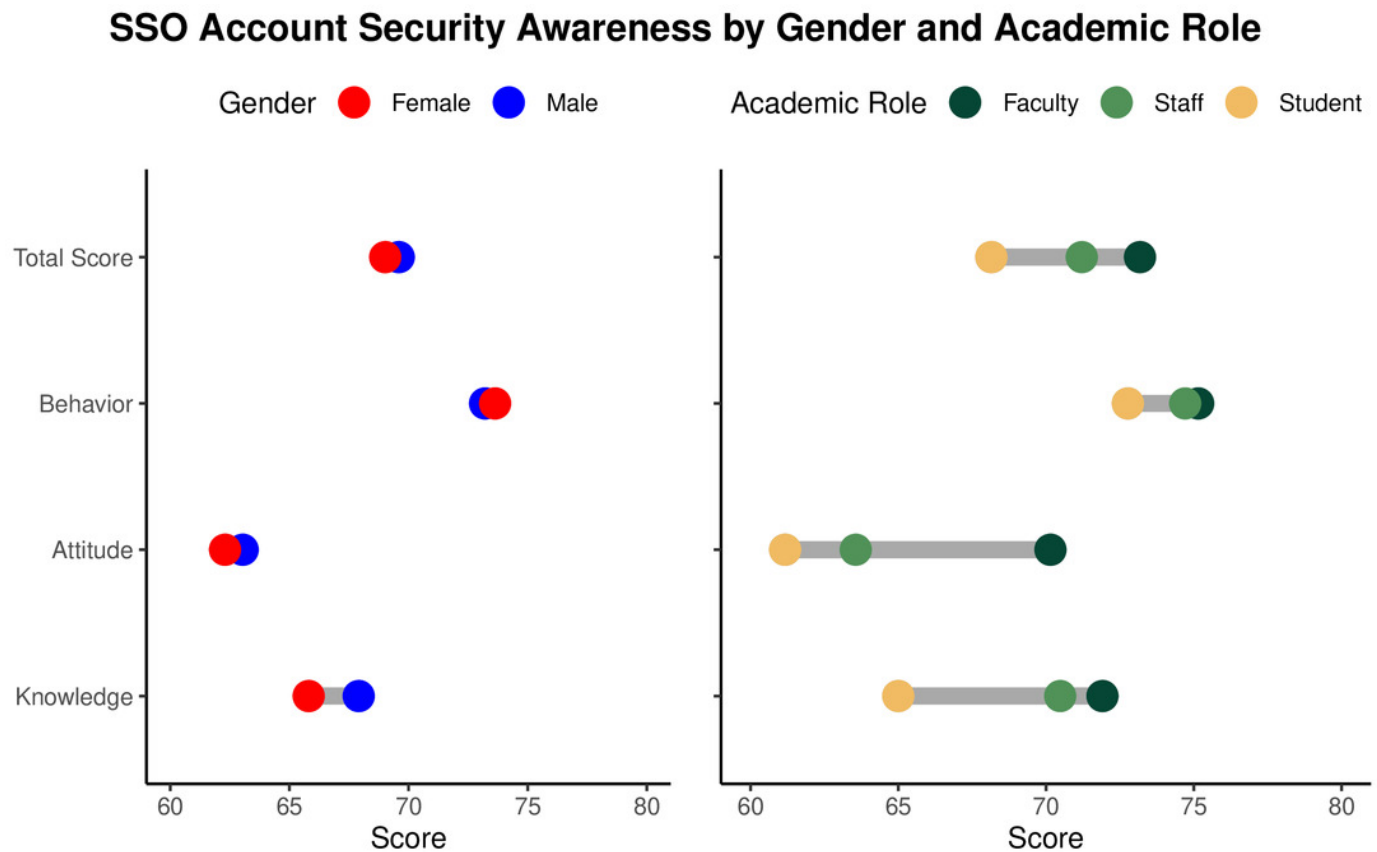
Figure 4

Marginal effects of the interaction terms between Big-Five personality traits and privacy concerns
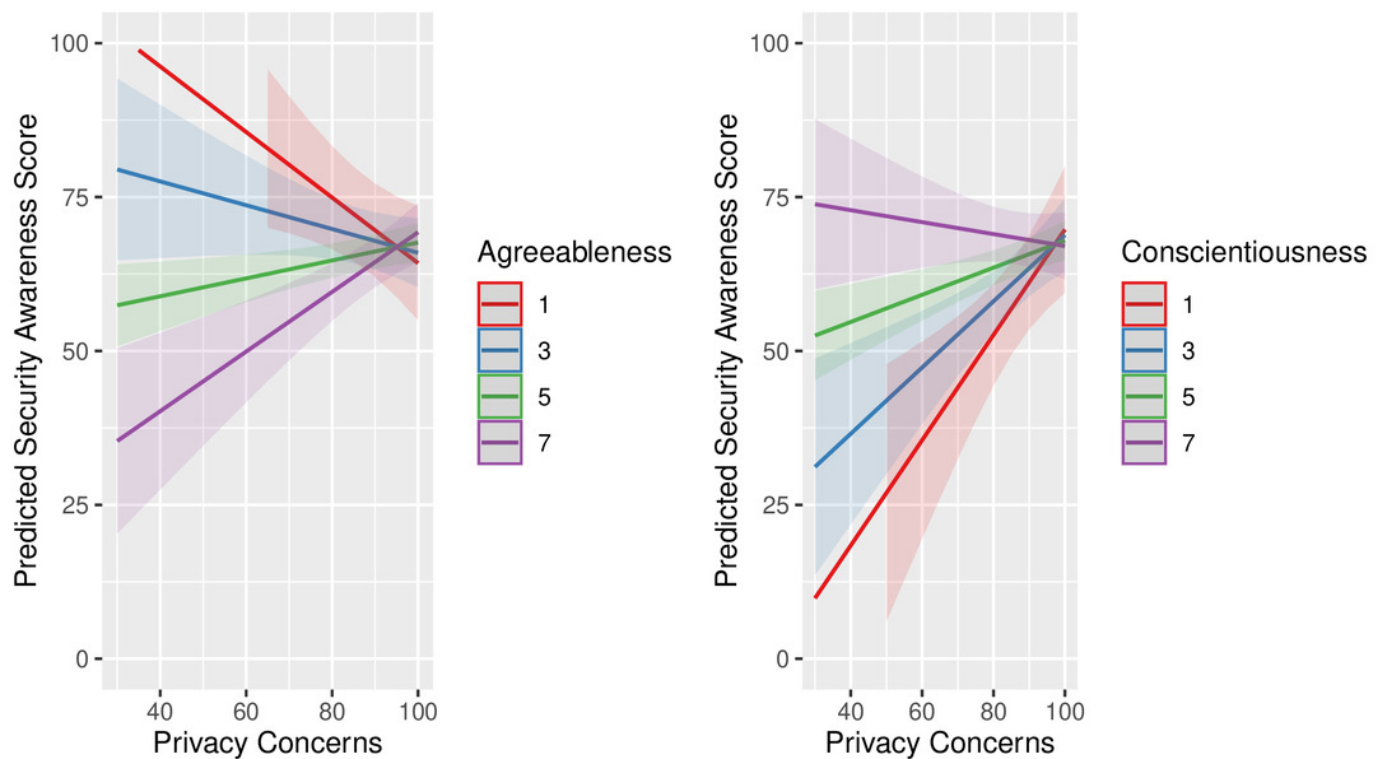
Figure 5

The final model of SSO account security awareness in this study

* students compared to faculty members;

Solid line indicates statistically significant relationship at p < .05;

Dotted line indicates not statistically significant relationship was found;

Numbers reported are the unstandardized coefficient (top) and the standardized coefficient (bottom)